Regolamento 679/16 - Sicurezza del Trattamento dei dati personali.

Adeguatezza delle misure e responsabilità dei fornitori - Prime considerazioni

Avv. Manuel Galdo – Foro di Milano

Con la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea del **Regolamento 679/16,** relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali, viene riformata la disciplina attualmente vigente: quali ripercussioni attendersi?

Se è pur vero che il Regolamento, in vigore dal 25 maggio 2016, prevede l'effettiva applicazione a decorrere dal 25 maggio 2018, lasciando così due anni di tempo ai soggetti interessati per adeguarsi alla nuova disciplina, appare non di meno necessario coglierne fin da subito la portata.

Tra le novità introdotte, merita attenzione quanto previsto all'**articolo 32**, poiché definisce una disciplina decisamente rilevante per chi dovrà confrontarsi professionalmente, in modo diretto o indiretto, con le problematiche connesse al trattamento dei dati personali.

Tale articolo prevede l'obbligo, per il **titolare** e per il **responsabile del trattamento**, di adottare "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*" e individua specifici rischi cui "*in special modo*" riferirsi (rischi derivanti dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trattati); nonché un'elencazione di misure "minime" da garantire.

Con un occhio particolare alle ricadute nell'ambito della sicurezza, dove il trattamento dei dati in discussione permea quasi l'intero settore (si pensi alla videosorveglianza, alla biometria, al controllo accessi,_solo per citare qualche esempio), l'esplicito riferimento fatto dalla norma al titolare e al responsabile del trattamento, non porti a ritenerla di poco momento per tutti gli altri soggetti che operano nel settore.

Oltre alle valutazioni che seguono, è lo stesso Regolamento a esplicitare, nel Considerando n. 78, come il titolare del trattamento dovrebbe attuare misure in linea con la nuova disciplina "*fin dalla progettazione*" e prosegue, a maggior chiarezza, affermando:

"*in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati*".

A ciò si aggiunga come la norma europea spingerà il titolare del trattamento ad essere sempre più attento alla necessità di reperire prodotti, servizi e installazioni che gli **garantiscano il rispetto degli obblighi su di lui gravanti** e, quindi, da un lato si **rivolgerà a chi tali garanzie saprà offrire** e, dall'altro, **pretenderà specifiche tutele contrattuali.**

Come detto, la disciplina in discussione non individua in modo tassativo le misure da adottare per rendere sicuro il trattamento dei dati, ma impone che queste siano *adeguate*.

Tale termine viene riferito sia alle misure da porre in essere per garantire la sicurezza, che ai rischi con cui confrontarsi: dunque, una doppia adeguatezza.

Prodotti e servizi utilizzati per il trattamento dei dati dovranno garantirne la sicurezza e rispondere alle esigenze introdotte con il Regolamento, e diverranno obsoleti ove, con riferimento alle innovazioni tecnologiche, tale sicurezza non sarà più attuale.

Anche per **il fornitore e per l'installatore** sarà quindi indispensabile la specifica conoscenza della problematica e delle soluzioni che si possono offrire, ciò sia per rispondere alle esigenze del committente, sia per evitare possibili responsabilità personali.

Conoscenza che dovrà, del pari, essere adeguata, da un lato, e costantemente aggiornata, dall'altro.

La normativa in commento, per i soggetti tenuti al rispetto di tali "indefiniti obblighi", pone un'altra problematica.

Infatti, venendo sancito un mero scopo (la sicurezza del dato trattato) e lasciato "aperto" il modo per raggiungerlo, risulta che l'accertamento di fatto sull'adeguatezza delle soluzioni proposte e adottate non potrà che avvenire con verifica *ex post.*

In altre parole, se il dato è violato, se il rischio si concretizza, significa che la soluzione adottata non era adeguata.

E', ovviamente, una drastica semplificazione doverosa per i limiti di tempo e spazio consentiti da questa prima analisi ma, tra le possibili, appare la più aderente a quella che si rivelerà essere la disciplina una volta a regime.

L'adeguatezza di cui alla norma, se è vero che potrà essere verificata solo *ex post,* nel contenuto precettivo non potrà che essere valutata con il criterio della c.d. "prognosi postuma": ci si colloca mentalmente al momento in cui la misura di sicurezza è stata adottata (valutazione *ex ante*) e, tenuto conto di tutte le circostanze concrete conosciute e conoscibili, si valuta la sua attitudine a perseguire il fine di sicurezza posto come obiettivo.

Valutazione che, prescrive la norma, deve essere eseguita tenendo conto "*dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*".

Restano, quindi, come canone di riferimento per il giudizio di adeguatezza le conoscenze scientifiche che dovranno essere tenute presenti sia per l'individuazione delle misure da adottare a tutela dei dati trattati, sia per l'individuazione dei possibili rischi connessi al loro trattamento: le due analisi sono, evidentemente, connesse e tra loro dipendenti.

La norma, con un dato testuale innovativo, introduce una valutazione economica, contemperando così l'interesse alla tutela del trattamento con quello dell'economicità della misura e, dunque, può dirsi che la miglior tecnologia possibile che dovrà essere applicata sarà quella, però, "economicamente sostenibile" (e pretendibile) in relazione alla – semplificando - diversa "importanza" dei dati trattati e del tipo di trattamento.

Sempre al fine di circoscrivere la responsabilità di chi si trovi a trattare i dati oggetto di tutela e/o per innescare circoli virtuosi e, quindi, innalzare il livello delle garanzie offerte nel trattamento dei dati personali, la norma stabilisce che la dimostrazione dell'adeguatezza delle misure, potrà essere dimostrata dall'aver aderito ad un codice di condotta o a un meccanismo di certificazione disposti in conformità a quanto stabilito dal Regolamento stesso (agli artt. 40 e 42).

In altre parole, l'accertata assenza di tale adesione porterà più facilmente ad affermare l'inadeguatezza delle misure adottate.

Questa è una previsione che merita particolare attenzione, poiché in tal senso, quindi, anche **l'essersi rivolto a un produttore, a un fornitore, a un installatore "diligente e preparato" sarà, per il responsabile, circostanza doverosa e che potrà essere spesa in chiave esimente da responsabilità.**

E', quindi, verosimile prevedere come codici di condotta, meccanismi di certificazione, protocolli o analoghe formule "certificative" saranno in tal senso necessarie, o quanto meno consigliabili, anche per gli stessi produttori, fornitori e installatori.

La norma in commento, come detto, ponendo la sicurezza quale obiettivo che informa l'intera attività del trattamento dei dati personali, non può che essere interpretata in modo da prevedere la responsabilità di chi procede al trattamento non solo ove la sicurezza del dato sia stata violata, ma anche laddove tale sicurezza sia posta meramente in effettivo pericolo.

In altre parole, l'adozione di misure "non adeguate", anche ove concretamente non si sia (ancora) verificata alcuna violazione alla sicurezza dei dati trattati, sarebbe già di per sé mancata attuazione delle prescrizioni di cui alla norma e, come tale, essere fonte di responsabilità (se non altro, di un obbligo coercitivamente imponibile ad adottare la misura necessaria).

Indispensabile, allora, che ogni soggetto che intervenga nella filiera connessa con il trattamento dei dati valuti e conosca i rischi connessi alla particolare forma di utilizzazione del dato di volta in volta posta in essere nonchè gli strumenti e le misure esistenti e adottabili per elidere o minimizzare tali rischi.

Quanto sopra, a maggior ragione considerando che l'attuale sistema relativo al trattamento dei dati personali, e alle responsabilità derivanti, non subirà rivoluzioni e, quindi, la vigente inversione dell'onere probatorio, stabilita in detta materia, sopravviverà alla modifica legislativa (in tal senso, l'art. 82 del Regolamento).

Ciò significa che ove un soggetto lamentasse un danno derivante dalla violazione nel trattamento dei dati personali, non avrà anche l'onere di dimostrare l'errore o la colpa nel trattamento, ma sarà il titolare del trattamento a dover dar prova dell'adozione di misure adeguate e di adeguata valutazione dei rischi e, in generale, di aver osservato le prescrizioni stabilite dalla disciplina regolante la materia.

Del pari, **chi ha fornito i prodotti o i servizi, potrà essere chiamato a rispondere per una responsabilità contrattuale.**

Da questa sommaria lettura, quindi, può comunque ravvisarsi la necessità – confermata e rafforzata – di doveroso e costante aggiornamento tecnico-scientifico in capo agli operatori della sicurezza con riferimento ai rischi connessi al trattamento dei dati personali e alle misure tecniche e organizzative necessarie per prevenirli.

L'innalzamento del livello di tutela, se comporta inevitabilmente maggiori responsabilità, può essere un'indubbia opportunità per quei soggetti che per primi e meglio sapranno interpretare le esigenze derivanti dalla nuova normativa, e offrire al mercato una risposta… *adeguata*.

essecome
security&safety